Teléfono de AnyConnect VPN de la configuración con la autenticación certificada en un ASA

Contenido

Introducción

Este documento proporciona una configuración de muestra que muestre cómo configurar el dispositivo de seguridad adaptante (ASA) y los dispositivos del CallManager para proporcionar la autenticación certificada para los clientes de AnyConnect que se ejecutan en los Teléfonos IP de Cisco. Después de que esta configuración sea completa, los Teléfonos IP de Cisco pueden establecer las conexiones VPN al ASA que hacen uso de los Certificados para asegurar la comunicación.

Prerequisites

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Licencia superior de AnyConnect SSL
- AnyConnect para la licencia del teléfono del Cisco VPN

Dependiente sobre la Versión de ASA, usted verá “AnyConnect para el teléfono de Linksys” para la versión 8.0.x ASA o “AnyConnect para el teléfono del Cisco VPN” para la versión 8.2.x ASA o más adelante.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- ASA - Versión 8.0(4) o más adelante
- Modelos del teléfono del IP - 7942/7962/7945/7965/7975
- Teléfonos - 8961/9951/9971 con el firmware de la versión 9.1(1)
- Teléfono - Versión 9.0(2)SR1S - Skinny Call Control Protocol (SCCP) o más adelante
- Administrador de las Comunicaciones unificadas de Cisco (CUCM) - Versión 8.0.1.100000-4 o más adelante

Las versiones usadas en este ejemplo de configuración incluyen:

- ASA - Versión 9.1(1)
- Versión del CallManager 8.5.1.10000-26

Para una lista completa de teléfonos soportados en su versión CUCM, complete estos pasos:

1. Abra este URL: https:// *<CUCM IP del servidor Address>:8443/cucreports/systemReports.do*
2. Elija la **lista unificada de la función del teléfono CM > generan un nuevos informe > característica: Virtual Private Network**.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Llame por teléfono a los tipos de certificado

Cisco utiliza estos tipos de certificado en los teléfonos:

- Certificado instalado fabricante (MIC) - Los MIC se incluyen en 7941, 7961, y los Teléfonos IP de Cisco de un más nuevo modelo. Los MIC son los Certificados dominantes 2048-bit que son firmados por el Certificate Authority (CA) de Cisco. Cuando un MIC está presente, no es necesario instalar el certificado significativo a localmente - (LSC). Para que el CUCM confíe en el certificado MIC, utiliza los Certificados de CA instalados previamente CAP-RTP-001, CAP-RTP-002, y Cisco_Manufacturing_CA en su almacén de la confianza del certificado.
- LSC - El LSC asegura la conexión entre CUCM y el teléfono después de que usted configure el modo de la seguridad del dispositivo para la autenticación o el cifrado.El LSC posee la clave pública para el Cisco IP Phone, que es firmada por la clave privada de la función de proxy del Certificate Authority CUCM (CAPF). Éste es el método preferido (en comparación con el uso de los MIC) porque solamente los Teléfonos IP de Cisco que es manualmente aprovisionado de un administrador se permiten descargar y verificar el archivo CTL.**Note**:

Debido al riesgo de seguridad mayor, Cisco recomienda el uso de los MIC solamente para la instalación LSC y no para el uso continuo. Los clientes que configuran los Teléfonos IP de Cisco para utilizar los MIC para la autenticación de Transport Layer Security (TLS) o para cualquier otro propósito hacen tan por su cuenta y riesgo.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Note: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

Configuraciones

Este documento describe estas configuraciones:

- Configuración ASA
- Configuración del CallManager
- Configuración VPN en el CallManager
- Instalación del certificado en los Teléfonos IP

Configuración ASA

La configuración del ASA casi es lo mismo que cuando usted conecta una computadora cliente de AnyConnect con el ASA. Sin embargo, estas restricciones se aplican:

- El grupo de túnel debe tener un grupo-URL. Este URL será configurado en el CM bajo el gateway de VPN URL.
- La directiva del grupo no debe contener un túnel dividido.

Esta configuración utiliza un certificado previamente configurado y instalado ASA (uno mismo-firmado o otro vendedor) en el trustpoint del Secure Socket Layer (SSL) del dispositivo ASA. Para más información, refiérase a estos documentos:

- Configurar los Certificados digitales
- El ASA 8.x instala manualmente los Certificados del vendedor de las de otras compañías para el uso con el ejemplo de configuración del WebVPN
- ASA 8.x: Acceso VPN con el cliente VPN de AnyConnect que usa el ejemplo de configuración del certificado autofirmado

La configuración pertinente del ASA es:

```
ip local pool SSL_Pool 10.10.10.1-10.10.10.254 mask 255.255.255.0
group-policy GroupPolicy_SSL internal
group-policy GroupPolicy_SSL attributes
split-tunnel-policy tunnelall
vpn-tunnel-protocol ssl-client

tunnel-group SSL type remote-access
tunnel-group SSL general-attributes
address-pool SSL_Pool
```

```
default-group-policy GroupPolicy_SSL
tunnel-group SSL webvpn-attributes
authentication certificate
group-url https://asa5520-c.cisco.com/SSL enable

webvpn
enable outside
anyconnect image disk0:/anyconnect-win-3.0.3054-k9.pkg
anyconnect enable

ssl trust-point SSL outside
```

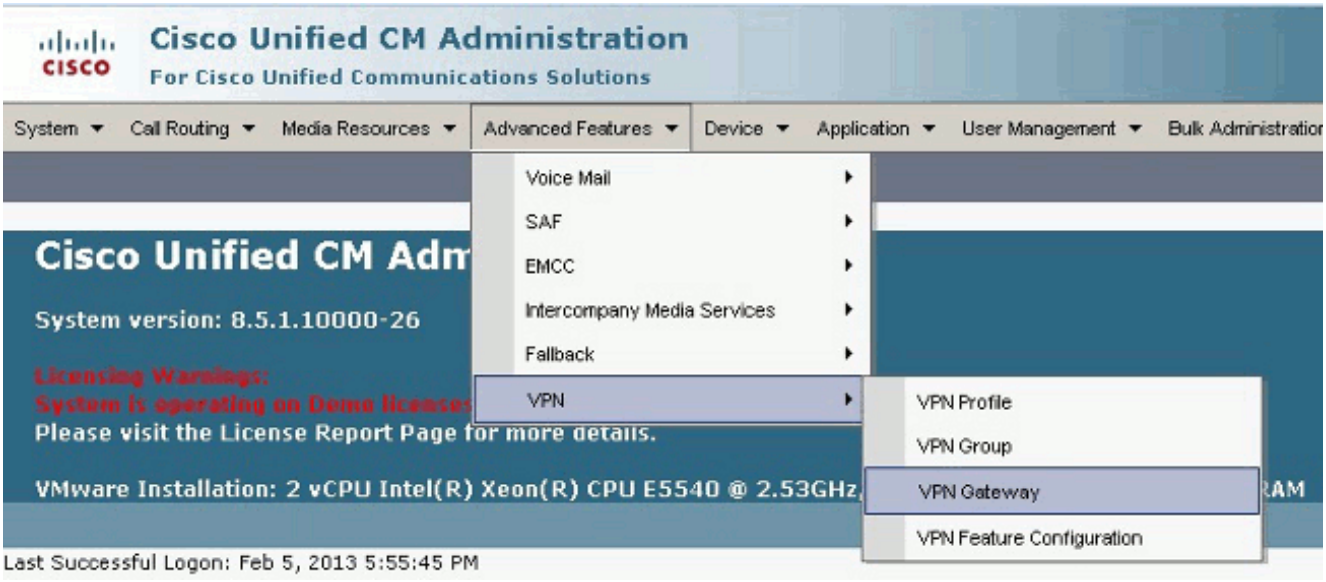
Configuración del CallManager

Para exportar el certificado del ASA e importar el certificado en el CallManager como certificado de la Teléfono-VPN-confianza, complete estos pasos:

1. Registre el certificado generado con CUCM.
2. Marque el certificado usado para el SSL.
   ```
   ASA(config)#show run ssl
   ssl trust-point SSL outside
   ```
3. Exporte el certificado.
   ```
   ASA(config)#crypto ca export SSL identity-certificate
   ```
   El certificado de identidad codificado Privacy Enhanced Mail (PEM) sigue:
   ```
   ASA(config)#crypto ca export SSL identity-certificate
   ```
4. Copie el texto de la terminal y sálvelo como archivo del .pem.
5. Inicie sesión al CallManager y elija el **Certificate Management (Administración de certificados) del > Security (Seguridad) de la administración OS > el certificado unificados de la carga > Teléfono-VPN-confianza selecta** para cargar el archivo de certificado guardado en el paso anterior.

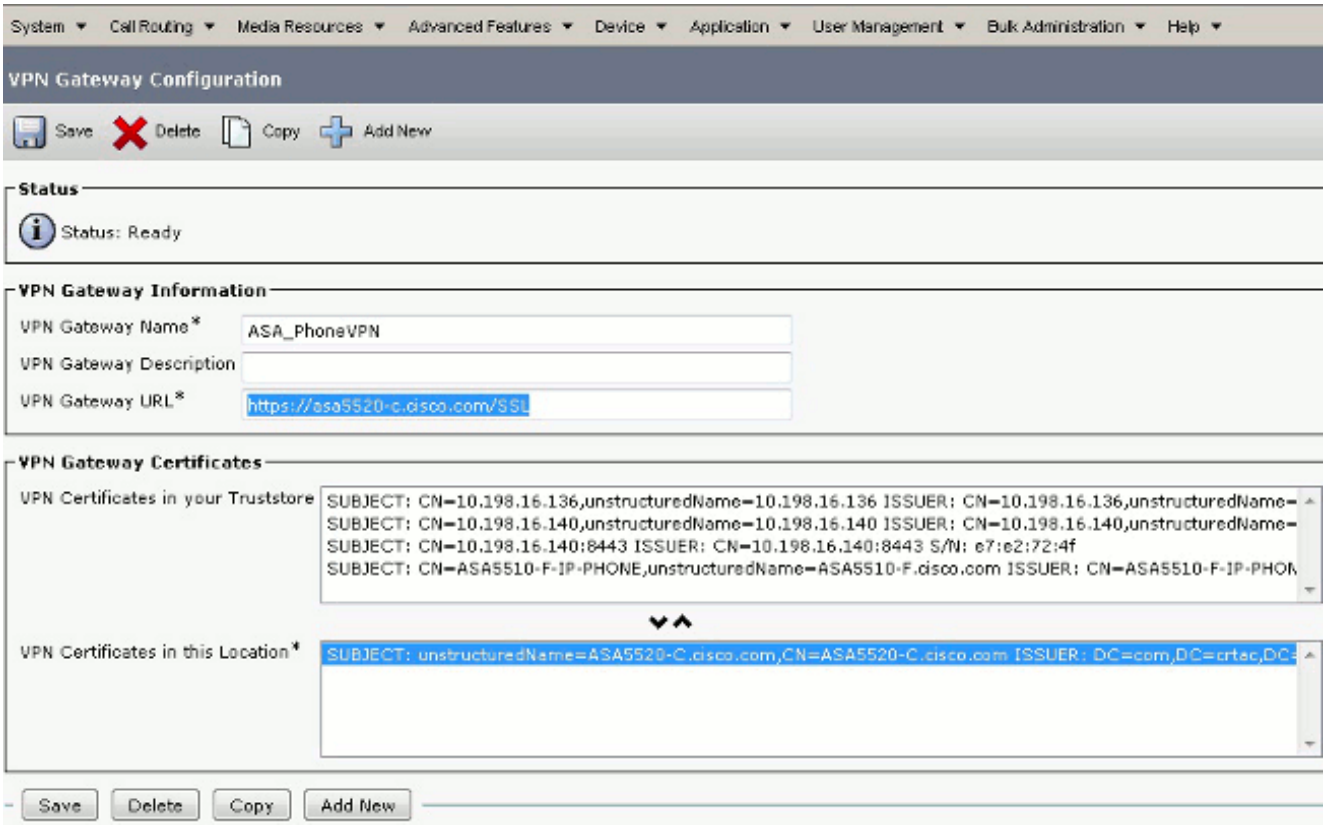
Configuración VPN en el CallManager

1. Navegue a Cisco unificó la administración CM.
2. De la barra de menú, elija las **funciones avanzadas > el VPN > el gateway de VPN**.

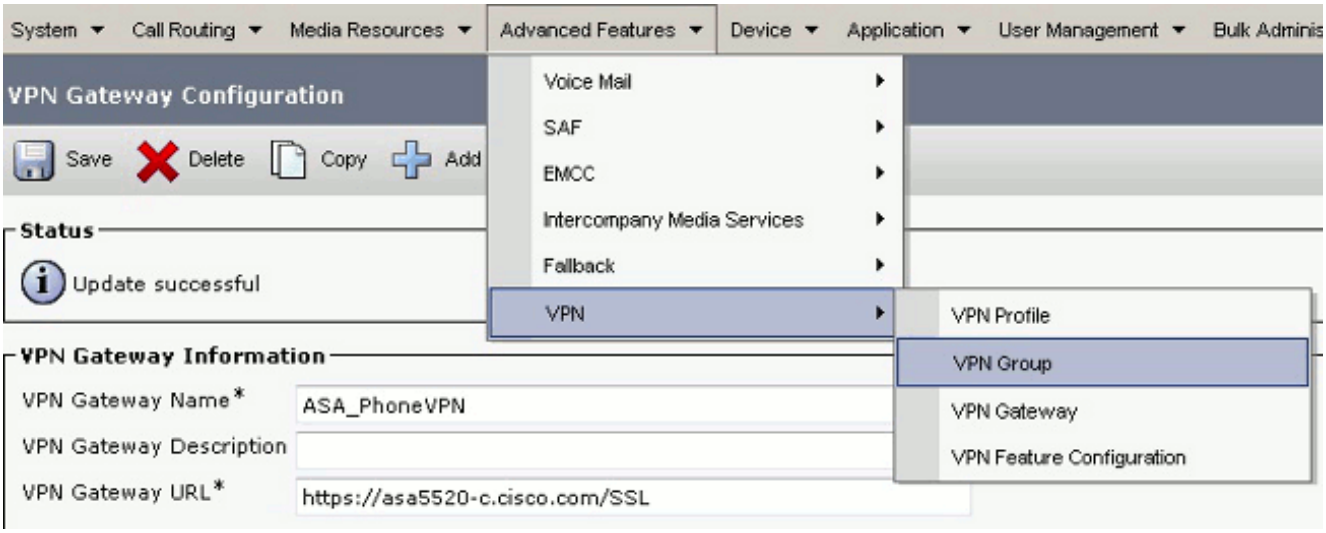


3. En la ventana de configuración del gateway de VPN, complete estos pasos:En el campo de nombre del gateway de VPN, ingrese un nombre. Éste puede ser cualquier nombre.En el campo Description (Descripción) del gateway de VPN, ingrese una descripción (opcional).En

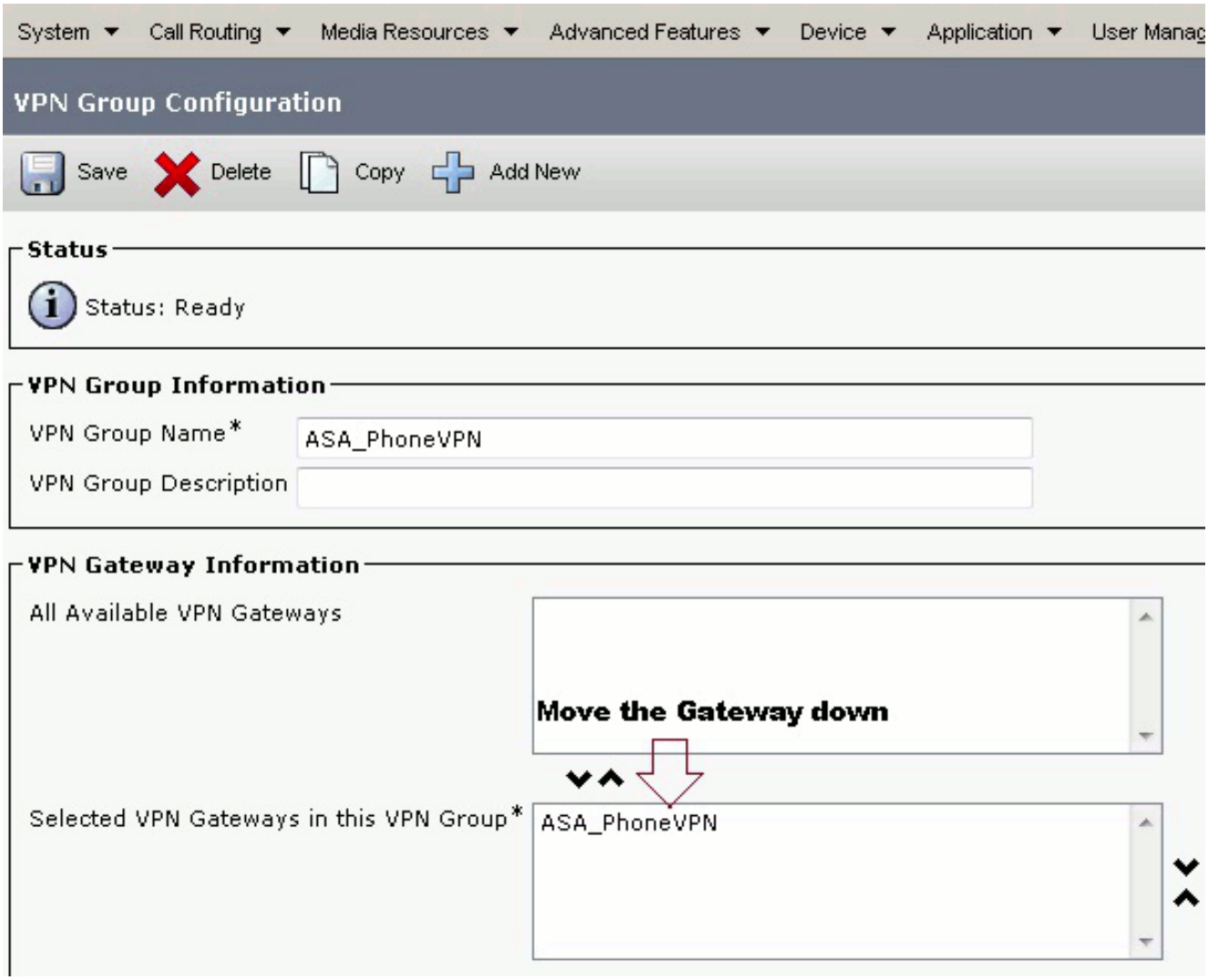
el campo URL del gateway de VPN, ingrese el grupo-URL definido en el ASA.En los Certificados VPN en este campo de la ubicación, seleccione el certificado que fue cargado al CallManager previamente para moverlo desde el truststore a esta ubicación.



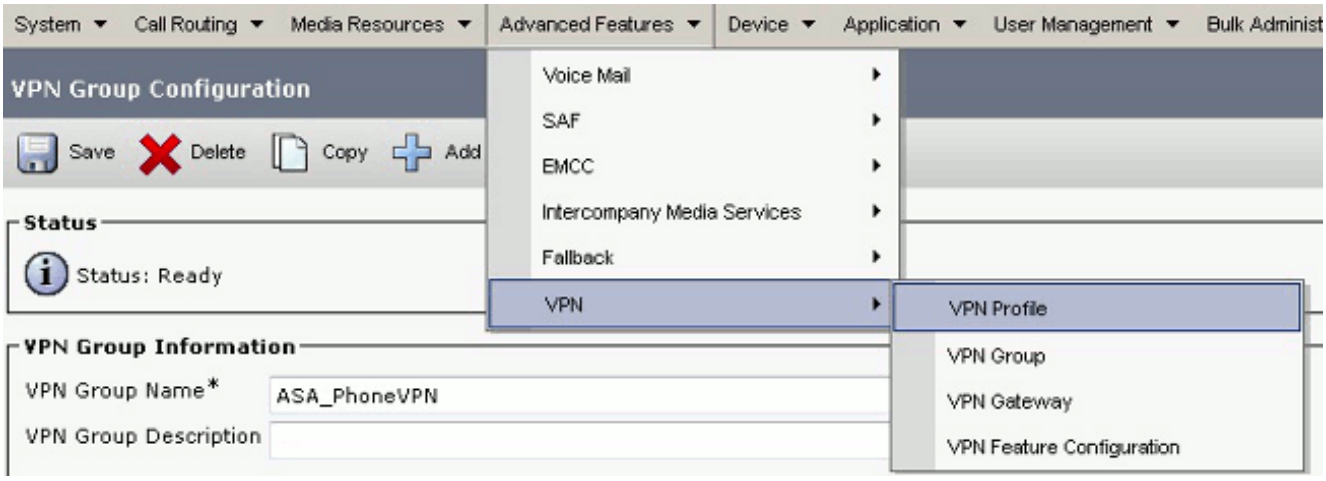
4. De la barra de menú, elija las **funciones avanzadas > el VPN > al grupo VPN**.



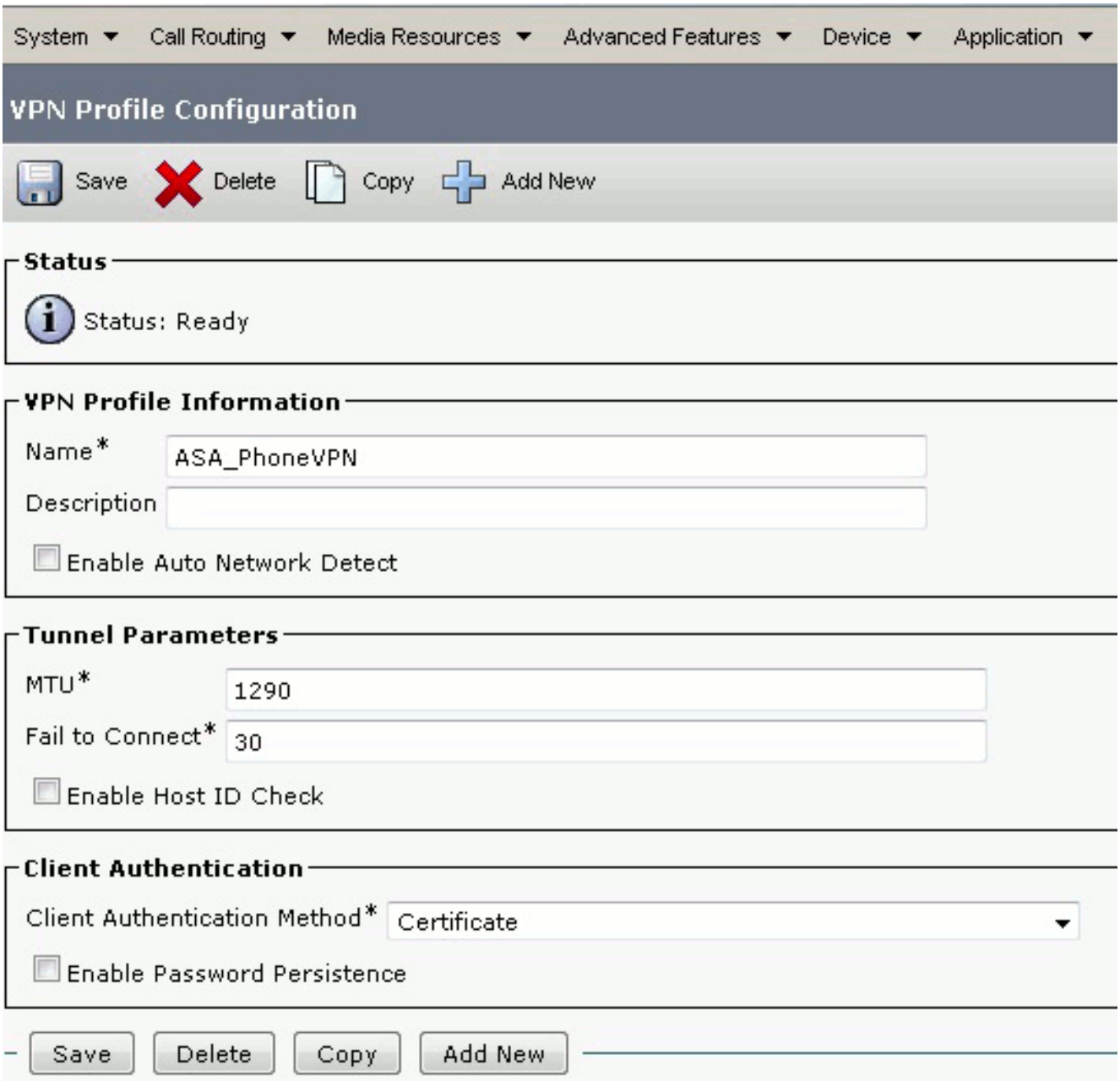
5. En todos los gateways de VPN disponibles coloque, seleccione el gateway de VPN definido previamente. Haga clic la flecha hacia abajo para mover el gateway seleccionado a los gateways de VPN seleccionados en este campo del grupo VPN.



6. De la barra de menú, elija las **funciones avanzadas > el perfil VPN > VPN**.

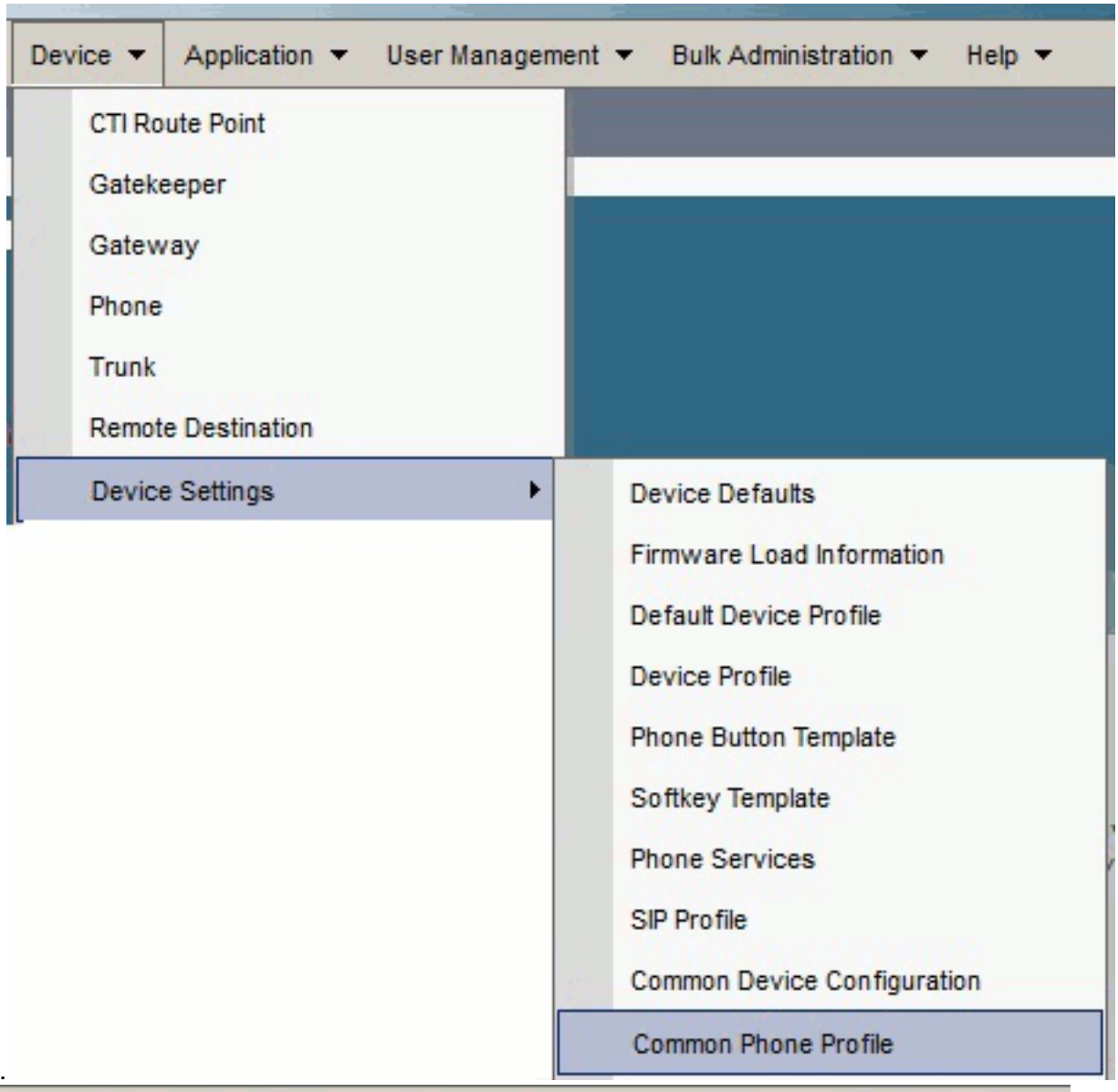


7. Para configurar el perfil VPN, complete todos los campos que se marquen con un asterisco (*).

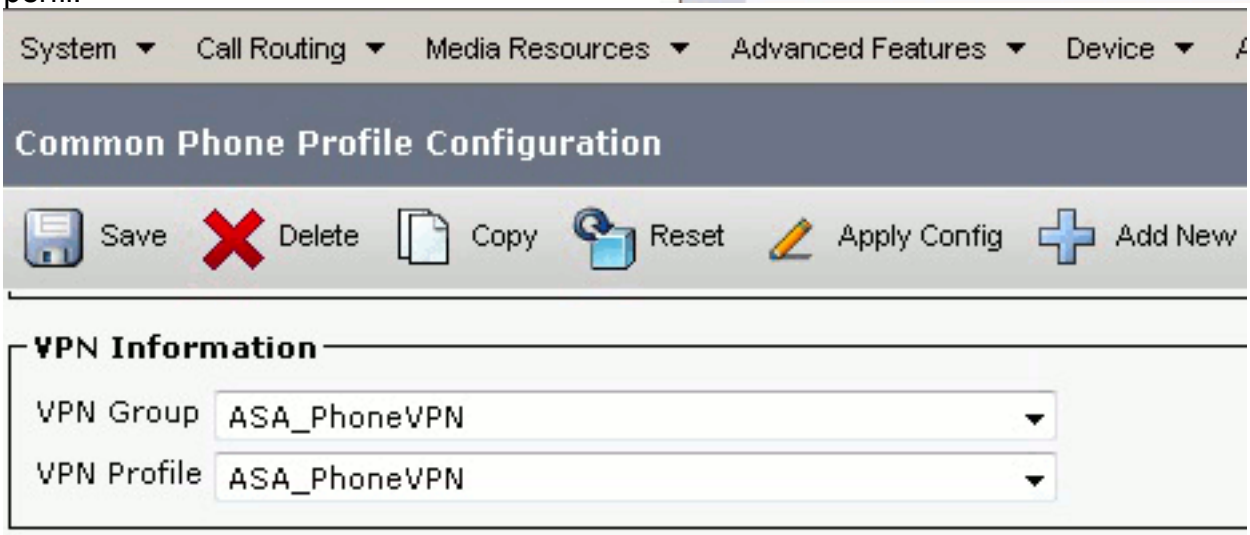


La red auto del permiso detecta: Si está habilitado, el teléfono VPN hace ping el servidor TFTP y si no se recibe ninguna respuesta, la los auto-iniciados una conexión VPN.**Control del ID del host del permiso:** Si está habilitado, el teléfono VPN compara el FQDN del gateway de VPN URL contra el CN/SAN del certificado. El cliente no puede conectar si no hacen juego o si un certificado del comodín con un asterisco (*) se utiliza.**Persistencia de la contraseña habilitada:** Esto permite que el teléfono VPN oculte el nombre de usuario y el passsword para la tentativa siguiente VPN.

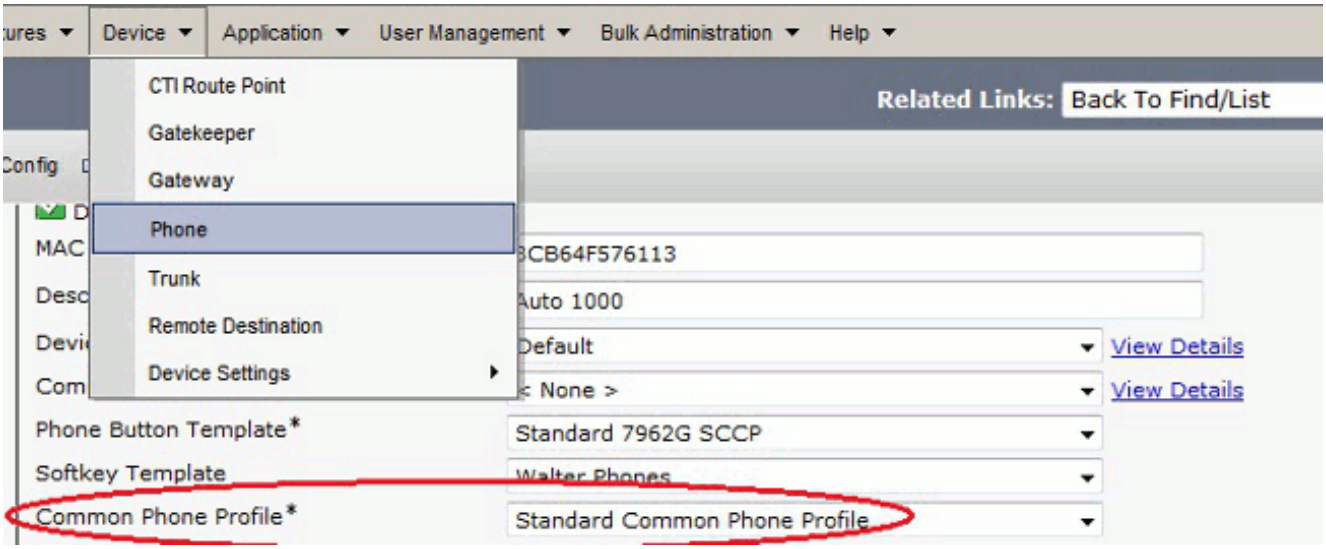
8. En la ventana común de la configuración del perfil del teléfono, el tecleo **aplica los Config** para aplicar la nueva configuración VPN. Usted puede utilizar “el perfil común del teléfono del estándar” o crear un nuevo



perfil.



9. Si usted creó un nuevo perfil para los teléfonos/los usuarios específicos, vaya a la ventana de la Configuración del teléfono. En el campo común del perfil del teléfono, elija el **perfil común del teléfono del estándar**.

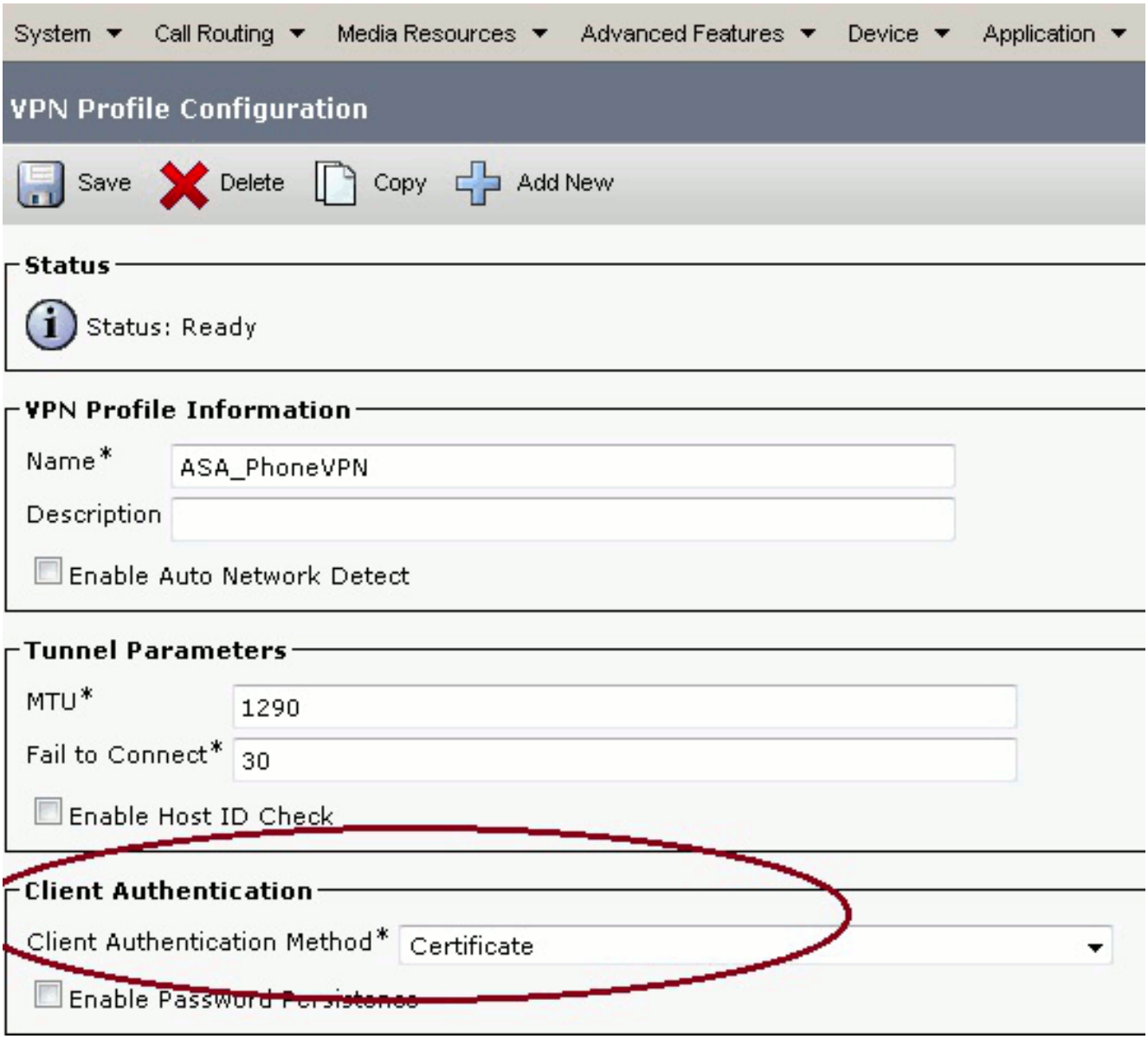


10. Registre el teléfono al CallManager otra vez para descargar la nueva configuración.

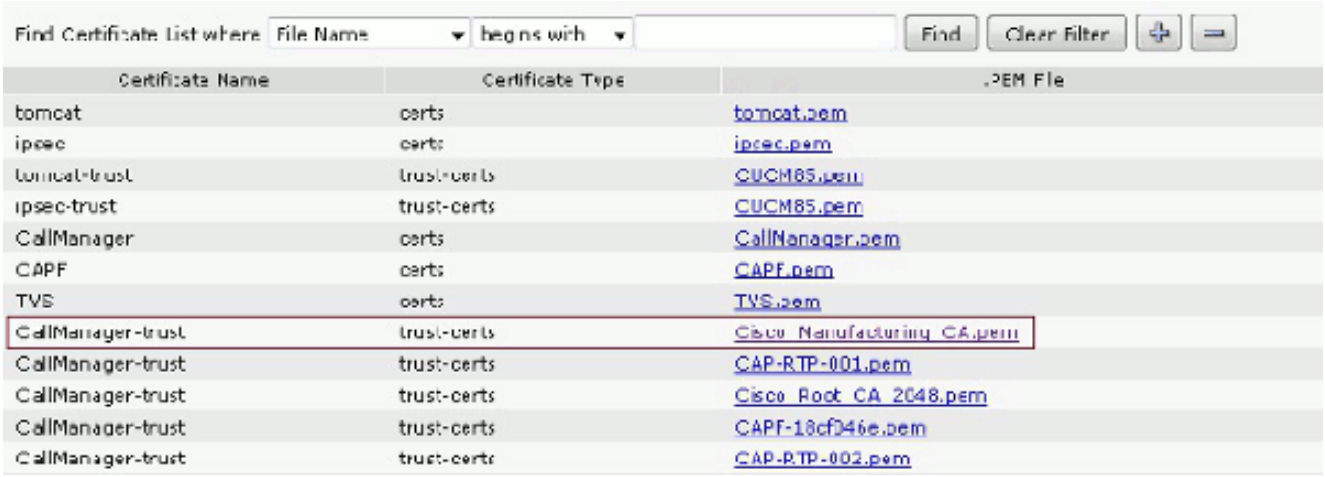
Configuración de la autenticación certificada

Para configurar la autenticación certificada, complete estos pasos en el CallManager y el ASA:

1. De la barra de menú, elija las **funciones avanzadas > el perfil VPN > VPN**.
2. Confirme el campo del método de autenticación de cliente se fija **para certificar.**



3. Inicie sesión al CallManager. De la barra de menú, elija el **Certificate Management (Administración de certificados) > el hallazgo unificados del > Security (Seguridad) de la administración OS**.
4. Exporte los certificados correctos para el método de autenticación certificada seleccionado:MIC: Cisco_Manufacturing_CA - Autentique los Teléfonos IP con un MIC



LSC: Función de proxy del Certificate Authority de Cisco (CAPF) - Autentique los Teléfonos IP con un

LSC

Certificate Name	Certificate Type	.PEM File	
tomcat	certs	tomcat.pem	tomcat.der
ipsec	certs	ipsec.pem	ipsec.der
tomcat-trust	trust-certs	CUCM85.pem	CUCM85.der
ipsec-trust	trust-certs	CUCM85.pem	CUCM85.der
CallManager	certs	CallManager.pem	CallManager.der
CAPF	certs	CAPF.pem	CAPF.der
TVS	certs	TVS.pem	TVS.der
CallManager-trust	trust-certs	Cisco_Manufacturing_CA.pem	

5. Encuentre el certificado, Cisco_Manufacturing_CA o CAPF. Descargue el archivo del .pem y sálvelo como archivo de .txt
6. Cree un nuevo trustpoint en el ASA y autentique el trustpoint con el certificado guardado anterior. Cuando le indican para el certificado de CA codificado base 64, selecto y pegue el texto en el archivo descargado del .pem junto con el COMENZAR y las líneas extremas. Se muestra un ejemplo a continuación:

```
ASA (config)#crypto ca trustpoint CM-Manufacturing
ASA(config-ca-trustpoint)#enrollment terminal
ASA(config-ca-trustpoint)#exit
ASA(config)#crypto ca authenticate CM-Manufacturing
ASA(config)#

<base-64 encoded CA certificate>

quit
```

7. Confirme la autenticación en el grupo de túnel se fija a la autenticación certificada.

```
tunnel-group SSL webvpn-attributes
authentication certificate
group-url https://asa5520-c.cisco.com/SSL enable
```

Instalación del certificado en los Teléfonos IP

Los Teléfonos IP pueden trabajar con los MIC o los LSC, pero el proceso de configuración es diferente para cada certificado.

Instalación MIC

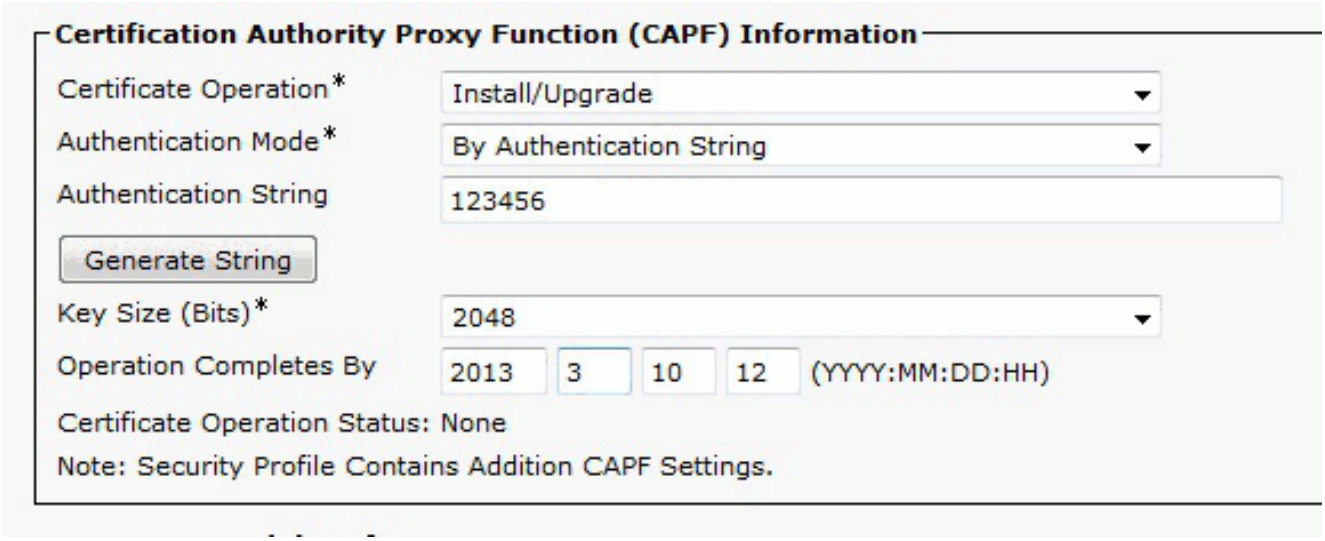
Por abandono, todos los teléfonos que soportan el VPN se cargan con los MIC. Los 7960 y 7940 teléfonos no vienen con un MIC, y requieren un procedimiento de la instalación especial para que el LSC se registre con seguridad.

Note: Cisco recomienda que usted utiliza los MIC para la instalación LSC solamente. Cisco soporta los LSC para autenticar la conexión TLS con CUCM. Porque los certificados raíz MIC pueden ser comprometidos, los clientes que configuran los teléfonos para utilizar los MIC para la autenticación de TLS o para cualquier otro propósito hacen tan por su cuenta y riesgo. Cisco no asume ningún defecto si se comprometen los MIC.

Instalación LSC

1. Servicio del CAPF del permiso en CUCM.
2. Después de que se active el servicio del CAPF, asigne las instrucciones del teléfono de generar un LSC en CUCM. Inicie sesión a Cisco unificó la administración CM y eligen el **Device (Dispositivo) > Phone (Teléfono)**. Seleccione el teléfono que usted configuró.
3. En la sección de información de la función de proxy del Certificate Authority (CAPF), asegúrese que todas las configuraciones estén correctas y la operación está fijada a una fecha

futura.



4. Si fijan al modo de autenticación a la cadena nula o al certificado existente, no se requiere ninguna otra acción.
5. Si fijan al modo de autenticación a una cadena, seleccione manualmente la **configuración del > Security (Seguridad) de las configuraciones > ** # > LSC > actualización** en la consola del teléfono.

Verificación

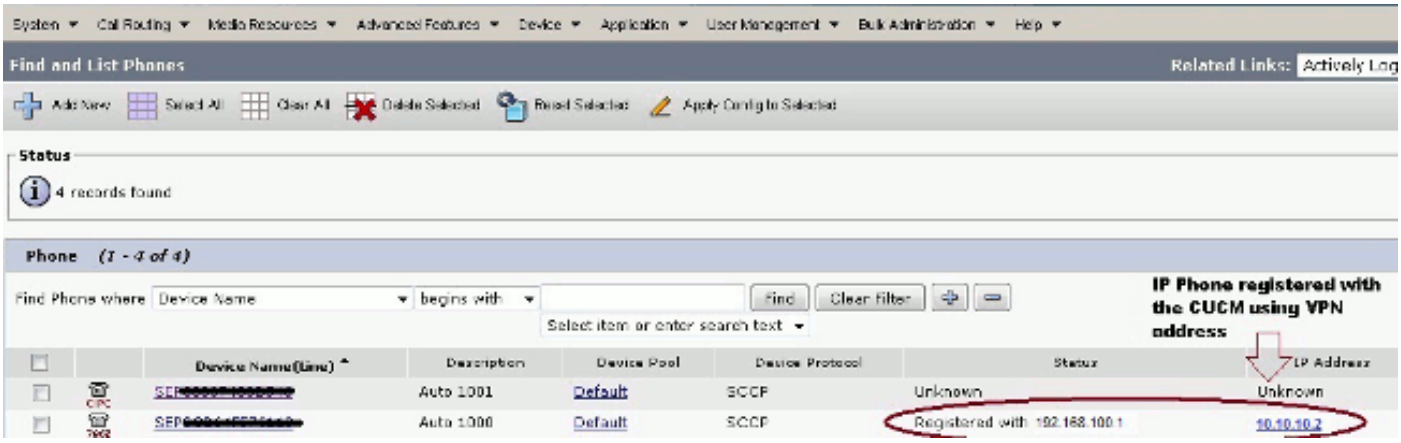
Utilize esta sección para confirmar que su configuración funcione correctamente.

Verificación ASA

```
ASA5520-C(config)#show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : CP-7962G-SEPXXXXXXXXXXXX
Index : 57
Assigned IP : 10.10.10.2 Public IP : 172.16.250.15
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium, AnyConnect for Cisco VPN Phone
Encryption : AnyConnect-Parent: (1)AES128 SSL-Tunnel: (1)AES128
DTLS-Tunnel: (1)AES128
Hashing : AnyConnect-Parent: (1)SHA1 SSL-Tunnel: (1)SHA1
DTLS-Tunnel: (1)SHA1Bytes Tx : 305849
Bytes Rx : 270069Pkts Tx : 5645
Pkts Rx : 5650Pkts Tx Drop : 0
Pkts Rx Drop : 0Group Policy :
GroupPolicy_SSL Tunnel Group : SSL
Login Time : 01:40:44 UTC Tue Feb 5 2013
Duration : 23h:00m:28s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
```

```
Tunnel ID : 57.1
Assigned IP : 10.10.10.2 Public IP : 172.16.250.15
Encryption : AES128 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Dst Port : 443
Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client Type : AnyConnect Client Ver : Cisco SVC IPPhone Client v1.0 (1.0)
Bytes Tx : 1759 Bytes Rx : 799
Pkts Tx : 2 Pkts Rx : 1
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 57.2
Public IP : 172.16.250.15
Encryption : AES128 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Src Port : 50529
TCP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client Type : SSL VPN Client
Client Ver : Cisco SVC IPPhone Client v1.0 (1.0)
Bytes Tx : 835 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 57.3
Assigned IP : 10.10.10.2 Public IP : 172.16.250.15
Encryption : AES128 Hashing : SHA1
Encapsulation: DTLSv1.0 UDP Src Port : 51096
UDP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client Type : DTLS VPN Client
Client Ver : Cisco SVC IPPhone Client v1.0 (1.0)
Bytes Tx : 303255 Bytes Rx : 269270
Pkts Tx : 5642 Pkts Rx : 5649
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

Verificación CUCM



Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Bug relacionados

- El Id. de bug Cisco CSCtf09529, agrega el soporte para la característica VPN en CUCM para

8961, 9951, 9971 teléfonos
- El Id. de bug Cisco CSCuc71462, Conmutación por falla del teléfono del IP VPN tarda 8 minutos
- Id. de bug Cisco CSCtz42052, soporte del teléfono del IP SSL VPN para no los números del puerto predeterminado
- El Id. de bug Cisco CSCth96551, no todos los caracteres ASCII se soporta durante el usuario de VPN del teléfono + el login de la contraseña.
- Id. de bug Cisco CSCuj71475, entrada TFTP manual necesaria para el teléfono del IP VPN
- Llamadas faltadas, puestas, o recibidas de la registración del Id. de bug Cisco CSCum10683, de los Teléfonos IP

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems